一种基于无证书签密技术的 NFC 移动支付方案 *

柳　毅，余　浩

(广东工业大学 计算机学院，广州 510006)

摘　要：针对现有的大部分 NFC 移动支付方案中存在的证书管理复杂、消费者隐私保护力度不大和运行效率不高等问题，结合无双线性对的无证书签密技术和匿名技术，提出了一个高效安全的 NFC 移动支付方案。该方案使用动态更新的匿名交易账户实现消费者匿名交易的同时实现了交易的不可链接性，商户作为消费者和移动支付服务提供商的通信桥梁，实现了消费者离线支付。分析结果表明，该方案提供了高安全性交易和高质量的个人隐私保护的同时实现了高效率的移动支付。

关键词：无证书签密技术；匿名技术；NFC 通信技术；消费者离线支付；安全支付；隐私保护

中图分类号：TP309.2　　doi: 10.3969/j.issn.1001-3695.2018.05.0350

NFC mobile payment scheme based on certificateless signcryption technology

Liu Yi, Yu Hao

(*School of Computer Guangdong University of Technology*, *Guangzhou* 510006, *China*)

Abstract: Most of the existing NFC mobile payment schemes have some problems such as complex certificate management, low consumer privacy protection and low operating efficiency, using the certificateless signcryption technology without bilinear pairing operations and the anonymous technology to propose an efficient and secure NFC mobile payment scheme. The scheme uses the dynamically updated anonymous trading account to realize the anonymous transaction of the consumer and the unlinkability of the transaction, the merchant acts as a bridge between the consumer and the mobile payment service provider, enabling the consumer to pay offline. The result shows that the scheme provides high-security transactions and high-quality personal privacy protection as well as high-efficiency mobile payments.

Key words: certificateless signcryption technology; anonymous technology; near field communication; the offline payment for the consumer; secure payment; privacy protection

0　引言

随着智能移动终端的普及和移动支付技术的快速发展，基于移动终端的支付方式开始逐渐取代传统支付方式（刷卡支付或者现金支付等）在支付市场中占据主导地位，根据 Analysys 易观发布的《中国第三方支付移动支付市场季度监测报告 2017 年第 2 季度》数据显示，2017 年第二季度，中国第三方支付移动支付市场交易规模达 230408.2 亿元人民币，环比增长 22.50%。其中支付宝 53.70%的占有率高居榜首，腾讯金融以 39.12%市场份额紧随其后。支付宝和微信支付所使用的移动支付技术主要是二维码支付技术，该支付技术易于实现，支付便捷，但容易受到虚假或恶意二维码的攻击，安全性较差。而 NFC 移动支付技术具有良好的保密性和安全性，即使在手机没有电的情况下依然可以进行支付，因此 NFC 移动支付技术是未来移动支付技术中最有前景的支付手段之一。

移动支付过程中，用户最关心的除了便捷性外就是安全性，而现阶段 NFC 移动支付中主要是使用传统密码技术实现交易数据的安全性和用户的身份合法性认证。此类技术不仅运算量大，而且基本都存在复杂的证书管理和秘钥托管问题。

文献[1]利用无证书签名技术和伪身份技术实现了移动支付中的身份认证和用户隐私保护，但该方案使用的无证书签名技术涉及到大量的双线对运算操作，时间开销大。文献[2]为 NFC 移动支付技术提出了一种基于双线性对运算操作的秘钥认证方案，该方案在认证过程中使用了大量的双线性对运算操作，增加了认证时间开销，同时由于交易过程中用户使用的是真实身份 ID，不能提供匿名支付功能，用户个人隐私得不到有效保护。文献[5]使用随机变化的匿名 ID 作为用户交易的身份，增加了用户交易过程中的隐私保护力度，但该匿名 ID 是由公钥、私钥和证书组成，存在证书的复杂管理问题。文献[6]给匿名交易账户 ID 设定了有效期和信用值，实现了用户匿名支付

收稿日期：2018-05-11；**修回日期：**2018-07-02　　**基金项目：**国家自然科学基金资助项目（61572144）；广东省科技计划资助项目（2016B090918125）

作者简介：柳毅（1976-），男，江苏连云港人，教授，博士，主要研究方向为网络与信息安全（71181185@qq.com）；余浩（1991-），男，硕士研究生，主要研究方向为网络与信息安全.

的同时也实现了交易信息的不可链接性，极大的提高了用户的隐私安全，但缺点是一旦超过有效期，需要用户自己重新申请新的匿名交易账户 ID 和虚拟银行账户 ID，便捷性受到影响。文献[7]使用了无双线性对的无证书签密技术实现了移动支付中用户的身份认证，极大的提高了身份认证效率，但该方案的交易记录对于发卡方来讲是透明的，且没有实现用户离线支付，一旦移动终端没有网络支撑，该方案无法完成交易，大大限制了交易场所的范围。文献[8]提出了一种基于 NFC 的用户匿名移动支付协议，用户用虚拟账户和虚拟交易账户进行交易，虚拟账户和虚拟交易账户都由用户自己产生，只有银行知道用户的真实身份，但需要用户每次交易完成后去更新他/她的虚拟账户来实现交易的不可链接性。

在 NFC 通信技术基础上，本文结合无双线性对操作运算的无证书签密技术和匿名技术提出一个身份认证效率高、隐私保护力度大和使用范围广的 NFC 移动支付方案。

1 相关工作

1.1 NFC 通信技术

NFC（near field communication）即近场通信，是由非接触式射频识别（RFID）演变而来，是在 RFID 技术基础上的一种扩展，工作频率为 13.56 MHz，传输距离为 10 cm[9]，传输速度为 106 kbps、212 kbps 和 424 kbps，一次只与一台设备连接，使用硬件安全模块进行加密，因此具有较好的保密性和安全性[10]。NFC 有三种工作模式：读写器模式、卡模拟模式和点对点模式[11]。因具有良好的便捷性和安全性，NFC 技术现已广泛应用在移动支付、电子票务、服务发现、数据交换、门禁系统和公交系统等。

1.2 无证书公钥密码技术

无证书公钥密码学概念是由 Al-Riyami 和 Paterson 在 2003 年的亚密会上提出的[12]。与基于 PKI（公钥基础设施）的传统公钥密码技术相比，无证书公钥密码技术和基于身份的密码技术一样不需要公钥证书，消除了公钥证书的复杂性管理问题，同时，在无证书公钥密码技术中，秘钥生成中心只是负责生成用户的部分秘钥，完整的秘钥是结合用户随机选取的秘密值生成的，且私钥由用户秘密存放，因此秘钥生成中心无法得知用户完整的私钥，从而克服了基于身份密码技术中私钥托管问题。可以说，无证书公钥密码技术是一种性能优良、运行效率高的公钥密码技术[13]。

公钥密码技术分为加密技术、签名技术、秘钥协商技术和签密技术。其中签密技术由 Zheng[14]提出，相对于对消息进行独立的加密和签名来讲，实现了加密和签名的同时降低了计算成本和通信开销。无证书公钥签密技术一般由以下七个算法[15]定义：

a）建立系统参数。KGC 输入安全参数 k，输出系统私钥 msk、系统公钥 mpk 和系统公开参数 $params$。

b）生成部分私钥。KGC 输入系统公钥 mpk，系统私钥 msk 和用户 U_A 的身份 ID_A，输出用户的部分私钥 d_A，并通过安全信道把 d_A 发送给用户 U_A。

c）生成秘密值。用户 U_A 选取个随机数 y_A 作为其秘密值。

d）生成私钥。用户 U_A 输入系统公钥 mpk、用户身份 ID_A、部分私钥 d_A 和秘密值 y_A，输出完全私钥 s_A。

e）生成公钥。用户 U_A 输入系统公钥 mpk、用户身份 ID_A、部分私钥 d_A 和秘密值 y_A，输出公钥 PK_A。

f）签密。输入系统参数 $params$、签密者身份 ID_A、接收者身份 ID_B、接收者公钥 PK_B、签密者公钥 PK_A、签密者完全私钥 s_A 和要签密的消息 m，输出密文 c。

g）解密验证。输入系统参数 $params$、签密者身份 ID_A、签密者公钥 PK_A、接收者身份 ID_B、接收者公钥 PK_B、完全私钥 s_B 和密文 c，如果验证通过，则输出明文消息 m，否则输出无效消息。

2 支付框架模型

本支付方案分为注册阶段和支付阶段，注册阶段分为消费者注册和商户注册两部分，消费者注册部分的参与方为消费者、移动支付服务提供商和可信第三方匿名生成中心，在这部分中，消费者在移动支付服务提供商处注册使用的匿名账户的合法性认证由可信第三方匿名生成中心提供。商户注册部分的参与方为商户、移动支付服务提供商和实名认证中心，在这部分中，商户身份合法性认证由实名认证中心提供。支付阶段的参与方有消费者、商户和移动支付服务提供商，消费者和商户提供相关信息给移动支付服务提供商，其中消费者提供的相关信息由商户进行转发，移动支付服务提供商提供身份认证和转账功能，若本次交易为大金额支付，消费者还需要输入支付口令才能顺利完成交易。图 1 为该方案的支付框架模型。

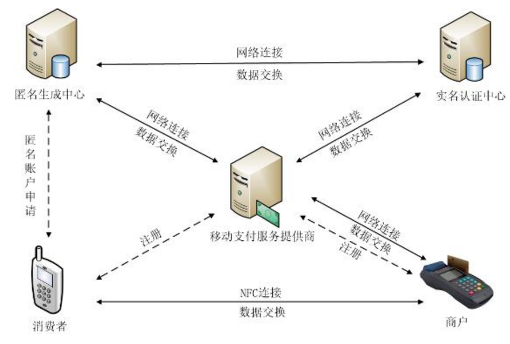


图 1 支付框架模型

3 方案描述

3.1 初始化系统参数

移动支付服务提供商在自己的云服务器上输入安全参数 k，产生两个大素数 p 和 q，且 $p-1$ 被 q 整除。G 为椭圆曲线上的一个循环群，P 为 G 上任意一阶为 q 的生成元。选取 3 个哈希函数：$H_1:\{0,1\}^*\times G\rightarrow Z_q^*$、$H_2:\{0,1\}^*\rightarrow Z_q^*$ 和 $H_3:G\rightarrow\{0,1\}^*$。选取一个随机数 $e\in Z_q^*$ 作为系统私钥并秘密保存在云服务器 SE 中，计算 $P_{pub}=eP$ 作为系统公钥。公开系统参数

$(p,q,P,P_{pub},H_1,H_2,H_3)$。

3.2 用户注册

3.2.1 消费者注册

消费者 C 通过移动终端上的 APP（由移动支付服务提供商 S 开发）进行注册，具体过程如下：

a）打开移动终端上的 APP，输入用户名 $username$、登录口令 lpw、支付口令 ppw、PIN 码、匿名账户 $AID_C(AID_C \in \{0,1\}^*)$ 和手机号码 PN 等注册信息，其中 AID_C 由可信第三方匿名生成中心生成，作为消费者在 S 处注册使用的唯一身份标志。计算 $H(username \| lpw)$、$H(PIN)$ 和 $H(ppw)$，保存 $H(username \| lpw)$ 到本地 SE 中，把 $H(ppw)$、AID_C 和 PN 通过安全信道发送给 S。

b）S 接收到 C 发来的注册信息后，根据 C 提供的手机号码发送短信验证码 SMS 给 C，确认该号码是否有效和本次注册申请是否是 C 本人操作。

c）C 在 APP 上输入短信验证码并发送给 S，S 把接收到的 SMS 与之前发送给 C 的短信验证码相比较，如果相同则把 AID_C 通过安全信道发送给匿名生成中心进行身份合法性认证，否则发送注册失败信息给 C。

d）匿名生成中心收到 S 发送过来的 AID_C，在自己的数据库中进行查找，若数据库中存在该匿名账户，则发送身份确认回执 $Confirm_C$ 给 S，否则发送认证失败信息给 S，S 再发送注册失败信息给 C。

e）S 对匿名生成中心发送过来的 $Confirm_C$ 进行辨别，如果是身份确认回执，则保存 $H(ppw)$ 和 AID_C 在本地 SE 中，并为 C 开通一个电子钱包，C 可以往电子钱包里进行充值，也可以进行提现操作。同时 S 生成匿名交易账户 $TAID_C \in \{0,1\}^*$ 和会话密钥 KEY，且 S 选择一个随机数 $r_{SC} \in Z_q^*$，计算 $R_C = r_{SC}P$ 和 $D_C = r_{SC} + eH_1(AID_C, R_C)$ 作为 C 的部分公钥和部分私钥，最后把生成的部分密钥、KEY 和 $TAID_C$ 通过安全信道发送给 C。

f）C 收到 S 发送过来的部分密钥后，计算等式 $R_C + H_1(AID_C, R_C)P_{pub} = D_C P$ 是否成立，若成立则接受部分密钥和 $TAID_C$，计算 $D = H_2(H(PIN)) \oplus D_C$，并把 D、KEY 和 $TAID_C$ 保存在本地 SE 中，同时删除 $H(PIN)$。否则发送密钥重申请求给 S 进行密钥重申操作。

具体注册流程如图 2 所示，本方案注册流程和支付流程中出现的符号，其解析如表 1 所示。

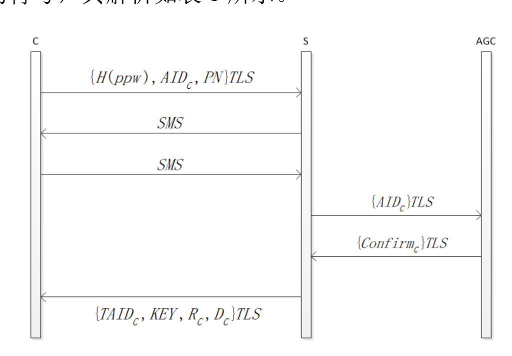


图 2　消费者注册流程

表 1　方案中符号解析

标志	描述
C	消费者
M	商户
S	移动支付服务提供商
ppw	支付口令
AID_C	消费者匿名账户
ID_M	商户的真实身份
$H()$	哈希函数
TLS	TLS 协议
SMS	短信验证码
$Confirm_X$	X 的身份确认信息
$TAID_C$	匿名交易账户
R_X	X 的部分公钥
D_X	X 的部分私钥
KEY	会话密钥
AM	商户注册验证码
AU	实名认证中心
AGC	匿名生成中心
$Token$	商户的身份标志
m	支付信息
(h_X, s_X) 或 (h_X', s_X')	X 生成的签名
C_X 或 C_X'	X 生成的密文
$\|$	连接运算符
$\oplus$	异或运算符

3.2.2 商户注册

商户 M 在 S 的官方网站上进行注册。

a）M 在注册界面中输入真实身份 ID_M、$IMSI$ 码、地址 $address$、电话号码 TN、电子邮箱 $email$ 和其他相关注册信息 $Others$，并通过安全信道发送给 S。

b）S 收到注册信息后，发送验证码 AM 给 M。

c）M 在验证码输入框输入验证码，发送给 S。

d）S 确认验证码的正确性，如果正确则将 ID_M 发送给实名认证中心 AU 进行身份合法性认证，若认证通过，AU 将发送身份确认回执 $Confirm_M$ 给 S，否则发送认证失败信息给 S，S 再发送注册失败信息给 M。

e）S 收到身份确认回执 $Confirm_M$ 后，计算 $Token = H(ID_M \| IMSI \| rand_M) \in \{0,1\}^*$，选取一个随机数 $rand_M \in Z_q^*$。接着随机选择一个 $r_{SM} \in Z_q^*$，分别生成 M 的部分公钥和部分私钥 $R_M = r_{SM}P$，$D_M = r_{SM} + eH_1(Token, R_M)$，并生成一个会话密钥 KEY，最后通过安全信道把部分密钥、KEY 和 $Token$ 发送给 M。

f）M 收到部分密钥后，验证部分私钥的正确性，并把部分密钥、KEY 和 $Token$ 保存到 SIM 卡里。

具体注册流程如图 3 所示。

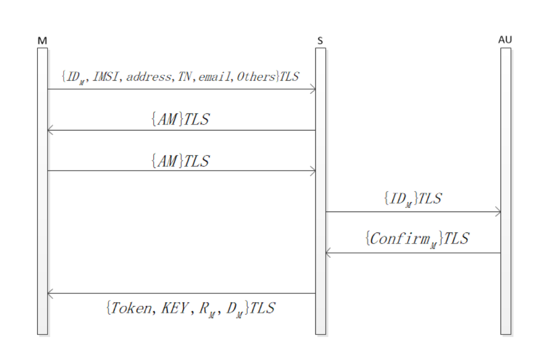


图 3　商户注册流程

3.3　身份认证

a)C 在 APP 登陆界面输入用户名 $username$ 和登录口令 lpw 打开支付功能并输入 PIN 码提取部分私钥：$D_C = H_2(H(PIN)) \oplus D$，同时提取 KEY 和 $TAID_C$。接着 APP 随机选择 $r_C \in Z_q^*$，计算 $Q_C = r_C P$，生成 C 的完全私钥 $SK_C = (r_C, D_C)$。APP 随机选择 $r_C^{'} \in Z_q^*$，计算 $T_C = r_C^{'} P$，$h_1 = H_1(ID_S, R_S)$。与此同时，M 从 SIM 卡中取出部分公钥 R_M、部分私钥 D_M、KEY 和 $Token$，选取一个随机数 $r_M \in Z_q^*$，计算 $Q_M = r_M P$，生成 M 的完全私钥 $SK_M = (r_M, D_M)$。接着再次选取一个随机数 $r_M^{'} \in Z_q^*$，计算 $T_M = r_M^{'} P$，$h_1 = H_1(ID_S, R_S)$，

$$h_M = H_2(T_M \| Token \| m), s_M = \frac{r_M^{'}}{r_M + D_M + h_M},$$

$V_M = r_M^{'}(Q_S + R_S + h_1 P_{pub})$，密文 $C_M = H_3(V_M) \oplus m$ 和密文 $\{m\}KEY$。

b）C 把移动终端靠近 M 的 POS 终端接收 M 发送过来的信息 $\{m\}KEY$，C 用刚才提取出的 KEY 来解密密文信息得到支付信息 m，计算 $h_C = H_2(T_C \| AID_C \| m)$，$s_C = \dfrac{r_C^{'}}{r_C + D_C + h_C}$，再从本地 SE 中取出 S 的公钥 $PK_S = (Q_S, R_S)$，算出 $V_C = r_C^{'}(Q_S + R_S + h_1 P_{pub})$，密文 $C_C = H_3(V_C) \oplus m$，最后把 $\{h_C, s_C, C_C, Q_C, TAID_C\}$ 发送给 M。

c）M 发送 C 的 $\{h_C, s_C, C_C, Q_C, TAID_C\}$ 和自身的 $\{h_M, s_M, C_M, Q_M, ID_M\}$ 给 S。

d）S 收到 M 发来的签密信息后，在数据库中查找 $TAID_C$ 对应的 AID_C 和 ID_M 对应的 $Token$，若存在则继续在本地 SE 中查找 AID_C 的部分公钥 R_C 和 ID_M 的部分公钥 R_M，结合发送过来的 Q_C, Q_M 可以得到 C 的完整公钥 $PK_C = (Q_C, R_C)$ 和 M 的完整公钥 $PK_M = (Q_M, R_M)$。接着计算 $h_1^{'} = H_1(AID_C, R_C)$，$V_S = s_C(r_S + D_S)(Q_C + R_C + h_1^{'} P_{pub} + h_C P)$，解密 C_C 得到 m= $C_C \oplus H_3(V_S)$，C_c 的具体解密过程如下：

$$V_S = s_C(r_S + D_S)(Q_C + R_C + h_1^{'} P_{pub} + h_C P)$$

$$= \frac{r_C^{'}}{r_C + D_C + h_C}(r_S + D_S)(r_C P + r_{SC} P + h_1^{'} eP + h_C P)$$

$$= \frac{r_C^{'}}{r_C + D_C + h_C}(r_S + D_S)(r_C P + D_C P + h_C P)$$

$$= r_C^{'} P(r_S + D_S)$$

$$= r_C^{'}(Q_S + r_{SS} P + eH_1(ID_S, R_S)P)$$

$$= r_C^{'}(Q_S + R_S + h_1 P_{pub})$$

由上述结果可以知道 $V_S = V_C$，因此 m= $C_C \oplus H_3(V_S)$ = $C_C \oplus H_3(V_C)$，明文恢复成功，同理可得到商户的明文。明文得到恢复后，S 比较来自消费者的 m 和来自商户的 m 是否相同，若相同则对两者进行身份认证操作，否则返回认证失败信息给消费者和商户并中断本次交易。C 的具体身份认证过程如下：

$$H_2(s_C(Q_C + R_C + h_1^{'} P_{pub} + h_C P) \| AID_C \| m)$$

$$= H_2(\frac{r_C^{'}}{r_C + D_C + h_C}(r_C P + r_{SC} P + h_1^{'} eP + h_C P) \| AID_C \| m)$$

$$= H_2(\frac{r_C^{'}}{r_C + D_C + h_C}(r_C P + D_C P + h_C P) \| AID_C \| m)$$

$$= H_2(r_C^{'} P \| AID_C \| m)$$

$$= H_2(T_C \| AID_C \| m)$$

$$= h$$

若上式成立，则身份认证通过。同理可认证商户 M 的身份。当两者身份都得到认证后，则接受支付信息 m。

3.4　支付交易

支付交易分两种情况，分别是小金额交易和大金额交易。

1)小金额交易

S 对消费者和商户完成身份认证后，将根据 m 上的相关支付信息进行转账，若 C 的电子钱包余额不足但开通了银行快捷支付，那么消费者可以选择使用银行快捷支付完成交易。若电子钱包和银行账户的余额都不足，或消费者没有选择银行快捷支付，那么此次交易失败，S 将发送交易失败信息给 C 和 M。

2)大金额交易

S 对消费者和商户完成身份认证后，发送 $\{h_S, s_S, C_S\}$ 给 M，其中 C_S 是支付口令请求信息的密文。C 确认 POS 终端上的支付金额正确后，在 POS 终端上输入支付口令 ppw，发送 $\{h_M^{'}, S_M^{'}, C_M^{'}\}$ 给 S，其中 $C_M^{'}$ 是 $H(ppw)$ 的密文。S 把收到的 $H(ppw)$ 与本地 SE 中的值对比，若相同，则执行与小金额支付同样的支付流程，否则终止本次交易，并发送交易失败信息给 C 和 M。

3.5　交易完成

交易成功后，S 发送 $\{h_{SM}^{'}, S_{SM}^{'}, C_{SM}^{'}, h_{SC}^{'}, S_{SC}^{'}, C_{SC}^{'}\}$ 给 M，其中 $C_{SM}^{'}$ 是 S 用 M 的公钥加密的支付成功回执的密文，而 $C_{SC}^{'}$ 是 S 用 C 的公钥加密的支付成功回执和新的匿名交易账户 $TAID_C^{'}$ 的密文。M 收到信息后，解密 $C_{SM}^{'}$ 得到支付成功回执并秘密存储，并把 $\{h_{SC}^{'}, S_{SC}^{'}, C_{SC}^{'}\}$ 发送给用户 C，C 解密 $C_{SC}^{'}$ 得到支付成功回执和 $TAID_C^{'}$ 并秘密存储到本地 SE 中，删除旧的 $TAID_C$，到此整个交易结束。

具体支付流程如图 4 所示（虚线表示只有大金额交易需要执行的步骤，实线表示大金额交易和小金额交易都必须要执行的步骤）。

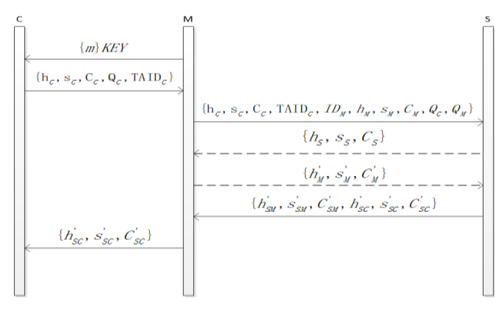


图 4　支付流程

4　安全性分析

4.1　抵抗数据窜改

M 和 C 之间传输的支付信息 m 通过会话密钥 KEY 进行加密，没有在 S 上注册的恶意用户在没有获得正确 KEY 的情况下无法解密获得正确的支付信息；若 C 是恶意用户，企图通过修改支付信息 m 来实现不正当交易，假设修改后的支付信息为 m'，因 S 在进行用户身份认证之前会先比较来自 C 的支付信息 m' 和来自 M 的支付信息 m，一旦发现 $m \neq m'$，则证明支付信息被恶意窜改，S 将终止本次交易；若 M 是恶意用户，在输入支付口令阶段，C 可以在商户的 POS 终端上确认 S 发送过来的支付金额是否合理，一旦发现支付金额有误，则可以直接拒绝在 POS 终端上输入支付口令，终止本次交易；假设攻击者冒充 S 接收签密信息，试图修改支付信息 m 来破坏本次交易，因攻击者无法获得 S 的私钥，故无法解密获得正确的支付信息 m，即无法对支付信息 m 进行修改。

4.2　抵抗假冒攻击

假设攻击者试图利用 C 的账户进行非法交易，因为攻击者无法得到 C 的手机，而 C 的部分私钥 D_C 只存储在 C 的手机中，所以攻击者无法获得正确的 D_C，即使攻击者得到了 C 的手机，但因 D_C 是以 $D = H_2(H(PIN)) \oplus D_C$ 的加密方式存储在手机中，攻击者在不知道 C 的 PIN 码的情况下，依然无法获得正确的 D_C。因此，攻击者试图通过使用伪造的 D_C' 进行交易。攻击者计算 $s_C' = \dfrac{r_C'}{r_C + D_C' + h_C}$，并通过 M 发送给 S，S 把 s_C' 代入以下等式进行身份认证：

$$
\begin{aligned}
&\text{因 } H_2(s_C'(Q_C + R_C + h_1'P_{pub} + h_CP) \| AID_C \| m) \\
&= H_2\Big(\frac{r_C'}{r_C + D_C' + h_C}(r_CP + r_{SC}P + h_1'eP + h_CP) \| AID_C \| m\Big) \\
&= H_2\Big(\frac{r_C'}{r_C + D_C' + h_C}(r_CP + D_CP + h_CP) \| AID_C \| m\Big) \\
&\neq h
\end{aligned}
$$

故身份认证失败，交易终止。

4.3　抵抗重放攻击

假设 M 是恶意用户，试图通过不断发送已经完成交易的签密信息给 S 来进行非法交易，但因为每次交易所使用的公私钥都不相同，故生成的签密信息也不相同，又因为上一次交易完成的签密信息依然保存在 S 的服务器上，一旦 S 发现此签密信息已存在于服务器上，则会直接丢弃此签密信息，因此本方案可以有效防护恶意商户的重放攻击。

4.4　身份匿名性

C 与 M 交易时使用的是 S 分发的匿名交易账户 $TAID_C$，所以 M 和攻击者都不能够从中获取 C 的真实身份，除此之外，C 在 S 中注册所使用的是匿名生成中心分发的匿名账户 AID_C，故 S 也不知道消费者 C 的真实身份，因此本方案充分地实现了消费者匿名交易，可以很好地保护消费者个人隐私。

4.5　不可否认性

当交易存在争议时，C 向 S 提供支付成功回执和匿名账户 AID_C 和 M 向 S 提供支付成功回执和真实身份 ID_M，S 根据支付回执中的订单号和交易时间在服务器上查找历史交易记录，然后验证历史交易记录中的交易金额和双方交易账户名与支付回执中的是否一致，若都一致，说明交易正常，若有其中一项不同，则说明交易存在异常。若两者有一方试图否认本次异常交易，但因历史交易记录中保存有双方的签名，因此不存在否认成功。

4.6　不可链接性

C 与 M 进行交易时使用的匿名交易账户 $TAID_C$ 在每次交易完成之后，都会进行更新，即实现了一次一户，即使 C 在同一家商店购买同样的商品，因交易时 C 使用的 $TAID_C$ 每次都不一样，因此 M 想获取 C 的真实身份是困难的。同时，因每次交易时 $TAID_C$ 的不同，M 无法把每次购买的商品信息与真正的 C 相关联，因此 M 企图利用商品属性推断出 C 的职业、兴趣爱好或者健康状况等相关个人隐私信息是困难的。同理，即使在 M 与 S 之间传输的加密信息被攻击者暴力破解了，攻击者也无法推断出 C 的相关个人隐私信息，实现了交易的不可链接性，很好的保护了消费者的个人隐私。

4.7　消费者离线支付

C 与 M 的数据交换是通过 NFC 技术进行的，而 M 又作为 C 和 S 之间的通信桥梁，因此 C 即使在没有网络的情况下依然可以顺利完成交易，即实现了消费者离线支付。

表 2 是本方案与文献[1,2]的安全性比较，其中 Y 代表可抵抗，N 代表不可抵抗。

表 2　安全性对比

安全属性	文献[1]	文献[2]	本方案
数据窜改	N	Y	Y
假冒攻击	Y	Y	Y
重放攻击	Y	Y	Y
身份匿名性	Y	N	Y
不可否认性	Y	Y	Y
不可链接性	Y	N	Y
消费者离线支付	Y	Y	Y

5　效率分析

本文采用文献[4]中的方法对各方案进行效率分析，根据文

献[1,3,4]的实验数据可以得到表 3 中的不同类型的密码操作时间开销，其中服务器端的时间开销是建立在 MIRACLE[16]密码库上的，服务器端搭配了一个 PIV 3 GHz 的处理器、内存为 512 MB 和使用 Windows XP 操作系统。客户端搭配了一个 206 MHz 的 ARM 处理器，使用 Linux 操作系统，在其上的各个密码操作时间开销是通过以下等式进行估算的：$t_C = t_S \times 3000/206$（$t_C$ 表示客户端的估计时间，t_S 表示服务器端的密码操作时间）。

表 3　不同类型密码操作时间开销　　/ms

密码操作类型	服务器端	客户端
双线性对上的标量积	6.38	92.91
椭圆曲线上的标量积	2.21	32.18
双线性对运算	20.04	291.84
双线性对上的幂运算	10.64	154.95

根据表 3 中各个密码操作时间开销可知，在文献[1]里，生成签名到完成身份认证整个过程中，客户端需要执行 1 次双线性对运算、2 次双线性对上的标量积运算和 2 次双线性对上的幂运算，而服务器端需要执行 2 次双线性对运算和 1 次双线性对上的幂运算，因此总的时间开销为 838.28 ms；在文献[2]里，客户端需要执行 5 次椭圆曲线上的标量积运算和 1 次双线性对运算，而服务器端需要执行 2 次椭圆曲线上的标量积运算和 1 次双线性对运算，因此总的时间开销为 477.2 ms；在本方案里，因为消费者和商户生成签名可以同时进行，因此客户端花费的时间为 3 次椭圆曲线上的标量积运算，而服务器端可以同时对消费者和商户的签名进行认证，所以服务器端的时间开销为 3 次椭圆曲线上的标量积运算，因此，总的时间开销为 103.17 毫秒。整个身份认证的过程需要在各个密码操作花费的时间如图 5 所示。

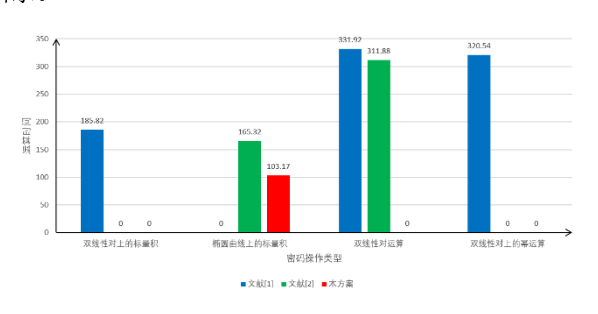


图 5　密码操作时间开销（以 ms 为单位）

文献[1,2]和本方案整个身份认证过程所需时间开销如表 4 所示。

表 4　时间开销　　/ms

方案	时间开销
文献[1]	838.28
文献[2]	477.20
本方案	103.17

根据表 4 可知本方案从生成签名到完成身份认证所需要的时间开销比文献[1]快了约 87.69%，比文献[2]快了约 78.38%，因此本方案效率更快，实用性更强。

6　结束语

本文结合无证书签密技术和匿名技术提出了一个安全高效的 NFC 移动支付方案，消费者部分私钥与其 PIN 码结合加密存储在移动终端中，增强了部分私钥防泄露属性；消费者与移动支付服务提供商进行通信使用的是可信第三方匿名生成中心分发的匿名账户，实现了消费者通信匿名；消费者与商户进行通信使用的是移动支付服务提供商分发的匿名交易账户，且该账户每次交易完后会得到更新，实现了匿名通信的同时也提供了交易的不可链接性，提高了消费者隐私安全；消费者每次交易都会使用新生成的私钥进行签名，实现一次一密，提高了身份认证的安全性，且具有抗重放攻击属性；消费者与移动支付服务提供商的信息交换是通过商户转发的，实现了消费者离线支付，扩大了交易场所的范围。分析结果表明，该方案提高了 NFC 移动支付安全性的同时很好的保护了消费者个人隐私，且提高了支付效率，是一种安全高效的移动支付方案。

参考文献：

[1] Qin Zhen, Sun Jianfei, Wahaballa A, *et al.* A secure and privacy-preserving mobile wallet with outsourced verification in cloud computing [J]. Computer Standards& Interfaces, 2017, 54: 55-60.

[2] Chen Xinyi, Choi K, Chae K. A secure and efficient key authentication using bilinear pairing for NFC mobile payment service [J]. Wireless Personal Communications, 2017, 97 (1): 1-17.

[3] He Debiao, Chen Jianhua, Zhang Rui. Efficient and provably-secure certificateless signature scheme without bilinear pairings. [J]. International Journal of Communication Systems, 2014, 25 (11): 1432–1442.

[4] Cao Xuefei, Zeng Xingwen, Kou Weidong, *et al.* Identity-based anonymous remote authentication for value-added services in mobile networks [J]. IEEE Trans on Vehicular Technology, 2009, 58 (7): 3508-3517.

[5] Eun H, Lee H, Oh H. Conditional privacy preserving security protocol for NFC applications [J]. IEEE Trans on Consumer Electronics, 2013, 59 (1): 153-160.

[6] Luo Jianing, Yang M H, Huang S Y. An unlinkable anonymous payment scheme based on near field communication [J]. Computers & Electrical Engineering, 2016, 49: 198-206.

[7] 王亚涛，赵波，陶威. 基于无证书公钥密码的 HCE 移动支付方案 [J]. 计算机工程与设计, 2017, 38 (1): 32-36. (Wang Yatao, Zhao Bo, Tao Wei. HCE mobile payment scheme on CL-PKC [J]. Computer Engineering and Design, 2017, 38 (1): 32-36.)

[8] Chen Shangwen, Tso R. NFC-based Mobile Payment Protocol with User Anonymity [C]// Proc of the 11th Asia Joint Conference on Information Security. n2016: 24-30.

[9] 贾凡，佟鑫. NFC 手机支付系统的安全威胁建模 [J]. 清华大学学报: 自然科学版, 2012, 52 (10): 1460-1464. (Jia Fan, Tong Xin. Threat modeling for mobile payments using NFC phones [J]. Journal of Tsinghua University

(Science and Technology) , 2012, 52 (10): 1460-1464.)

[10] 张玉清，王志强，刘奇旭，等. 近场通信技术的安全研究进展与发展趋势 [J]. 计算机学报，2016, 39 (6): 1190-1207. (Zhang Yuqing, Wang Zhiqiang, Liu Qixu, *et al.* Research progress and trends on the security of near field communication [J]. Chinese Journal of Computers, 2016, 39 (6): 1190-1207.)

[11] Rajesh G P, Pattar P, Divya M N, *et al.* Near field application: NFC smart notice board [C]// Proc of the 13th International Conference on Wireless and Optical Communications Networks. 2016: 1-5.

[12] 刘文浩，许春香. 无双线性配对的无证书签密方案 [J]. 软件学报，2011, 22 (8): 1918-1926. (Liu Wenhao, Xu Chunxiang. Certificateless signcryption scheme without bilinear pairing [J]. Journal of Software, 2011, 22 (8): 1918-1926.)

[13] 张福泰，孙银霞，张磊，等. 无证书公钥密码体制研究 [J]. 软件学报，2011, 22 (6): 1316-1332. (Zhang Futai, Sun Yinxia, Zhang Lei, *et al.* Research on Certificateless Public Key Cryptography [J]. Journal of Software, 2011, 22 (6): 1316-1332.)

[14] Zheng Yuliang. Digital signcryption or how to achieve cost (signature & encryption) ≪ cost (signature) +cost (encryption) [C]// Advances in Cryptology. Berlin: Springer, 1997, 1294: 165-179.

[15] Selvi S S D, Vivek S S, Rangan C P. Cryptanalysis of certificateless signcryption schemes and an efficient construction without pairing [C]// Proc of International Conference on Information Security and Cryptology. Berlin: Springer-Verlag, 2009: 75-92.

[16] Shamus Software Ltd. Miracl library [EB/OL]. [2018-05-10]. http://www.shamus. ie/index. php?page=home.